Parallel Repetition of entangled games on the uniform distribution

André Chailloux, Scarpa Giannicola

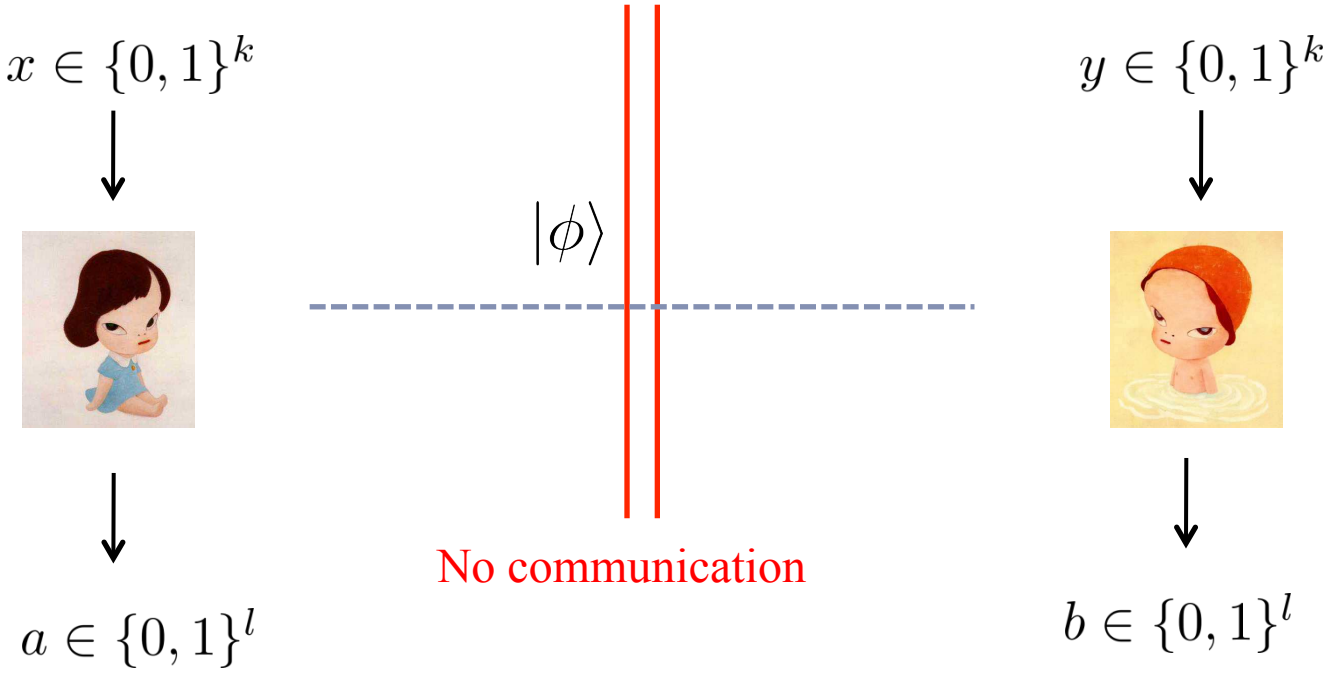
Parallel Repetition of entangled games on the uniform distribution

André Chailloux
INRIA Rocquencourt, Projet SECRET

Joint work with Giannicola Scarpa (CWI, Amsterdam)

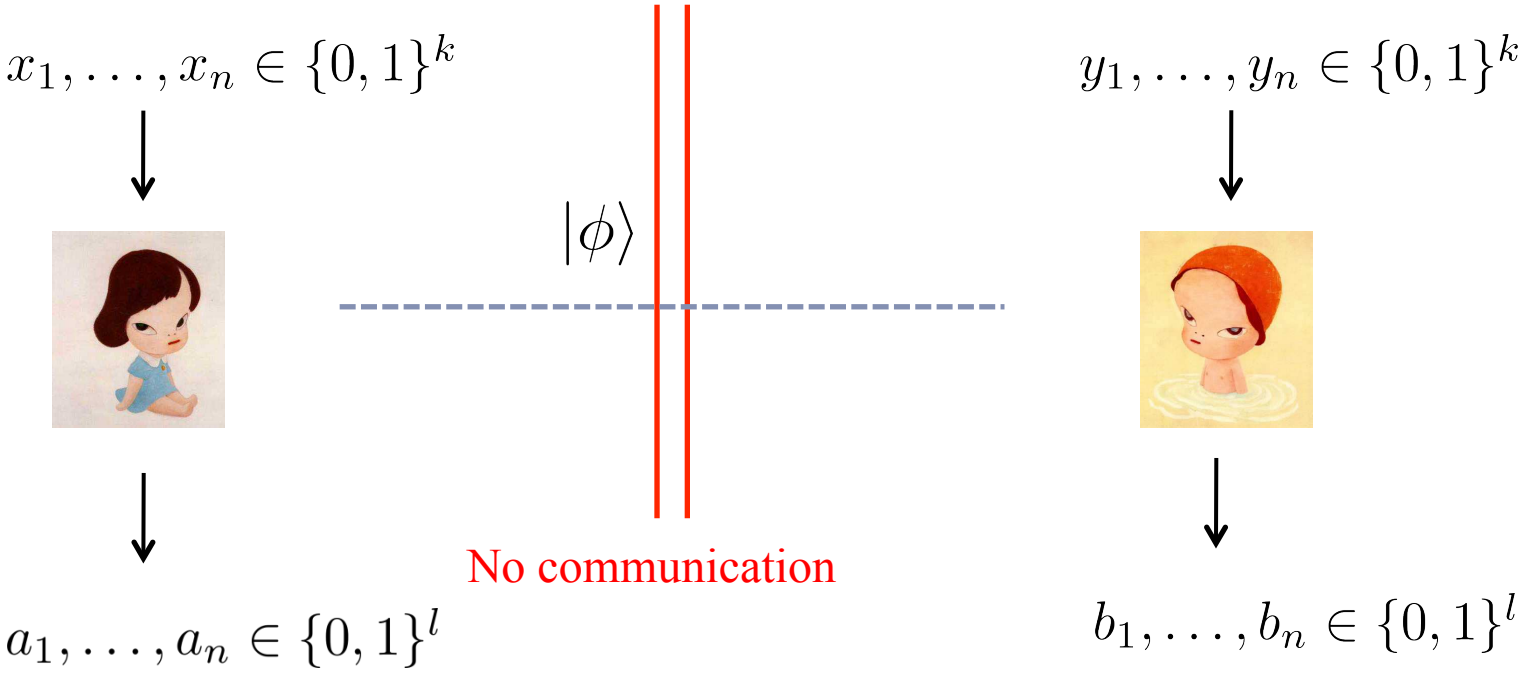
Nancy, JIQ 2013

Entangled games



- A game G = (V,p).
  - (x,y) is taken according to distribution p
  - Alice and Bob win the game if V(a,b|x,y) = 1
  - Max pr. of winning the game: $\omega^*(G)$

Parallel repetition



- Above game: G^n. Each (x_i, y_i) taken according to p.
- Alice and Bob win the game if $\forall i,\ V(a_i, b_i | x_i, y_i) = 1$
- Naive strategy: win wp. $(\omega^*(G))^n$
  - Possible to do better for some games.
  - What can we say about $\omega^*(G^n)$?

Why do we care ?

- Classically: widely used in complexity (hardness of approximation results)

- Quantumly
  - Natural object for studying non locality.
  - Helps understanding how to use entanglement efficiently
    - How can we do complicated stuff ?
  - Also related to hardness of approximation results.

Previous work

- Classically, widely studied.
- General games [Raz98] $\omega(G^n) \leq (1-\varepsilon^3)^{\Omega(n/l)}$ where $\omega(G) = 1-\varepsilon$
- Better results for specific kinds of games.

- Quantumly, also widely studied
  - XOR games[CleveSlofstraUngerUpadhyay06] (like CHSH): perfect parallel repetition : $\omega^*(G^n) = (\omega(G))^n$
  - Unique games[KempeRegevToner09]
  - General games [KempeVidick10] $\omega^*(G^n) \leq O(\frac{1}{n})$ when $\omega^*(G) = O(1)$

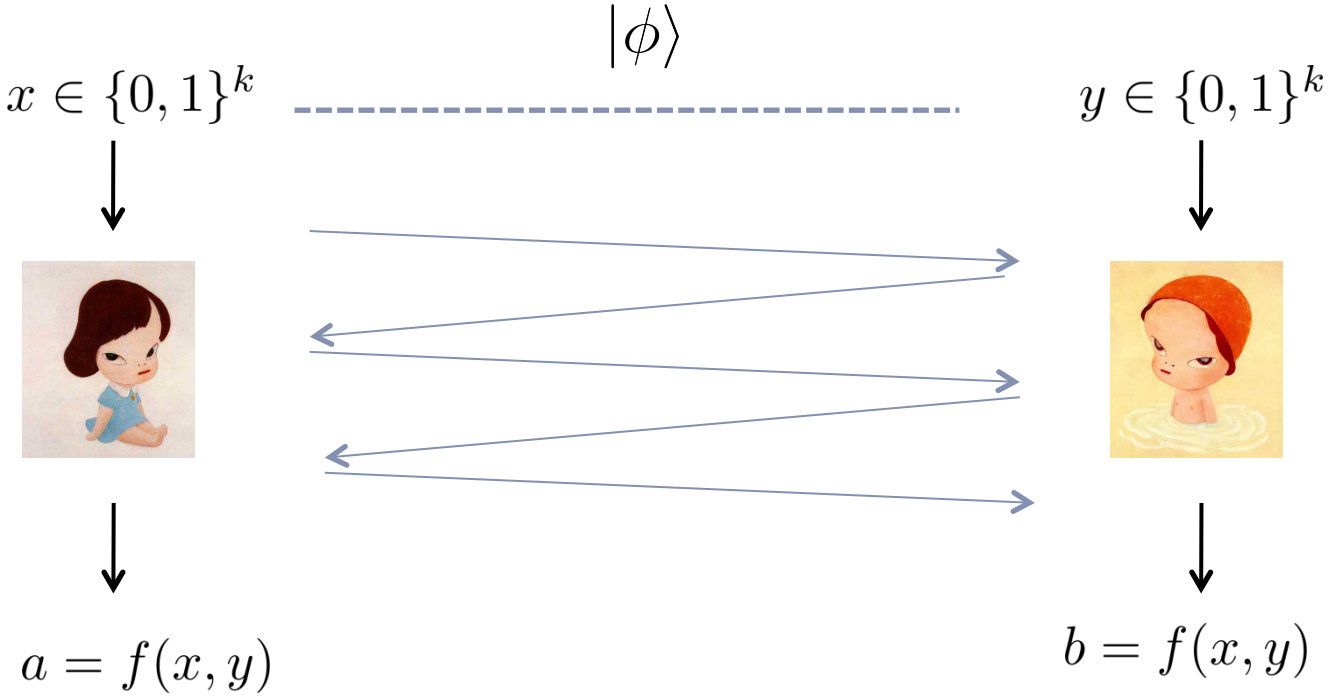
Our result

THEOREM

For any game G on the uniform distribution such that $\omega^*(G) \leq 1 - \varepsilon$, we have $\omega^*(G^n) \leq (1 - \varepsilon^2)^{\Omega(\frac{n}{kl})}$

- Main technique: extend the notion of Interactive Information Cost used in Communication complexity to entangled games.

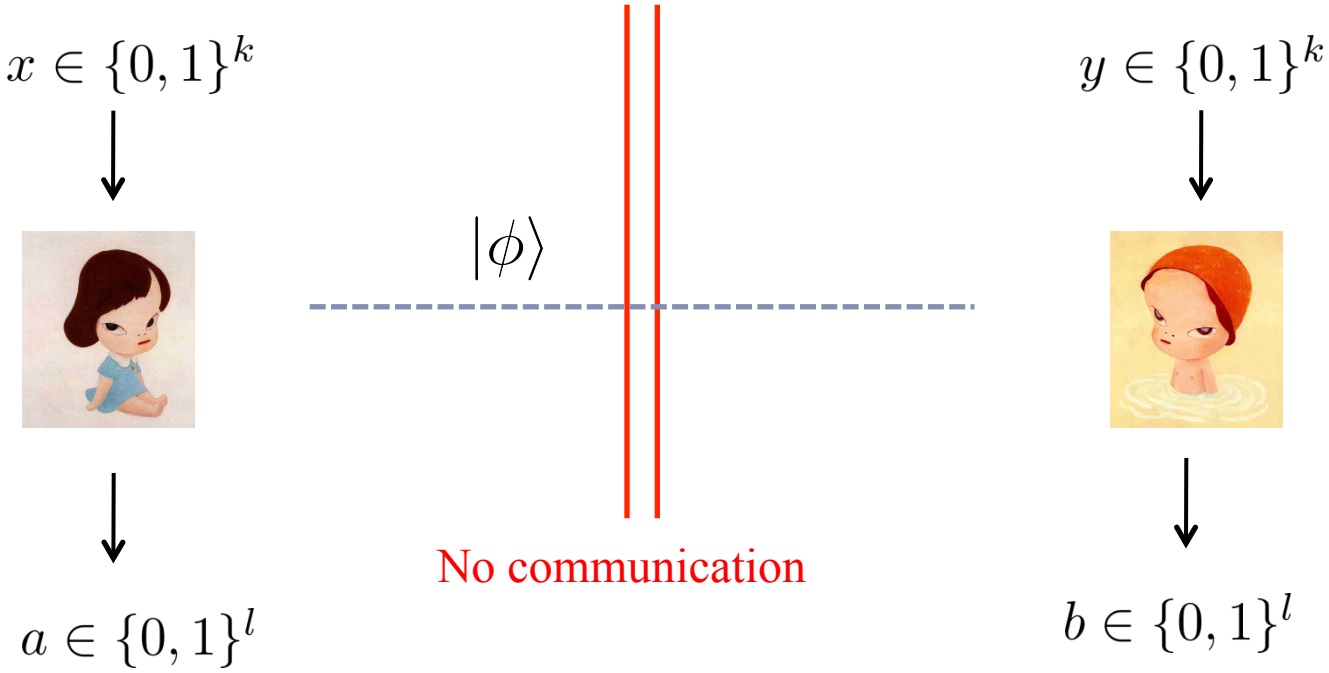
Information cost in communication complexity



- CC: minimal amount of communication in order to output f(x,y)
- IC: amount of information that Alice and Bob need to know about each other's inputs to output f(x,y)

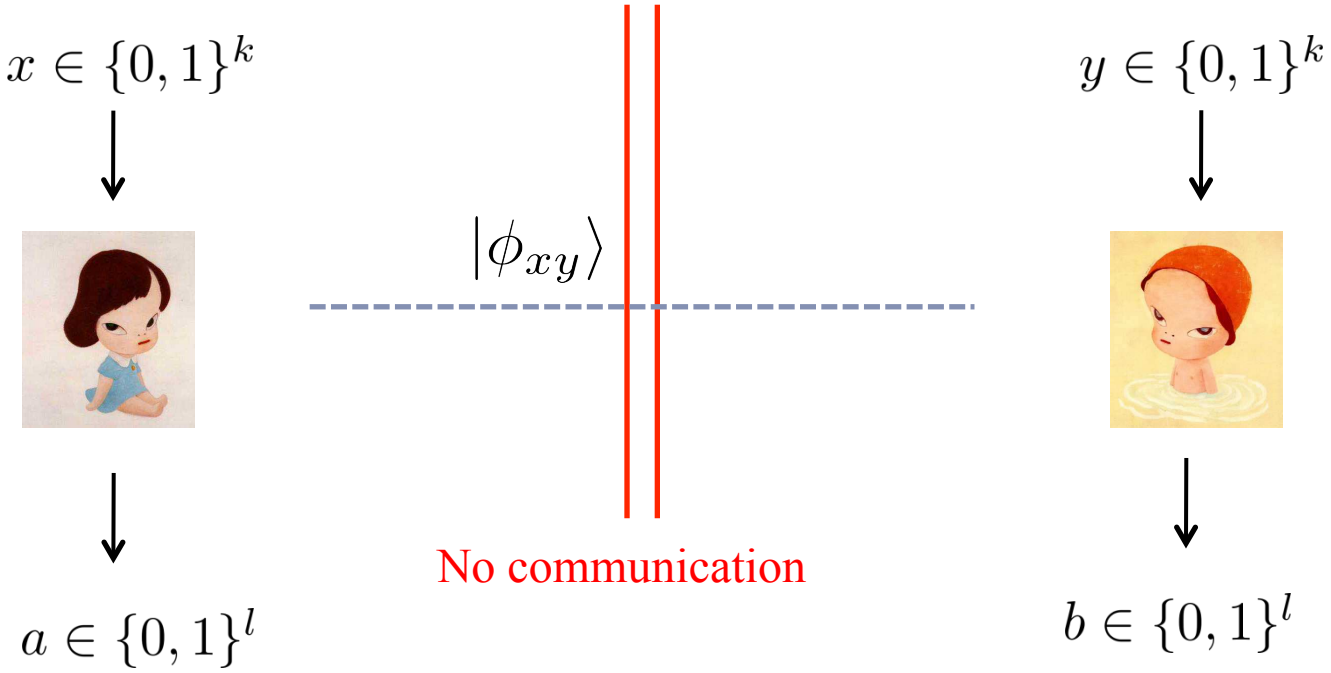
- IC is very cool when studying CC.
- Can we do the same for entangled games ?

Information Cost for Entangled games



- How to extend this to entangled games ?

Information Cost for Entangled games



- How to extend this to entangled games ?
- Advice states: the state Alice and Bob share can depend on x,y
- IC for games (informal def):

IC(G) = minimal amount of information that these states have to give to Alice & Bob about each other's inputs to win wp. 1 ?

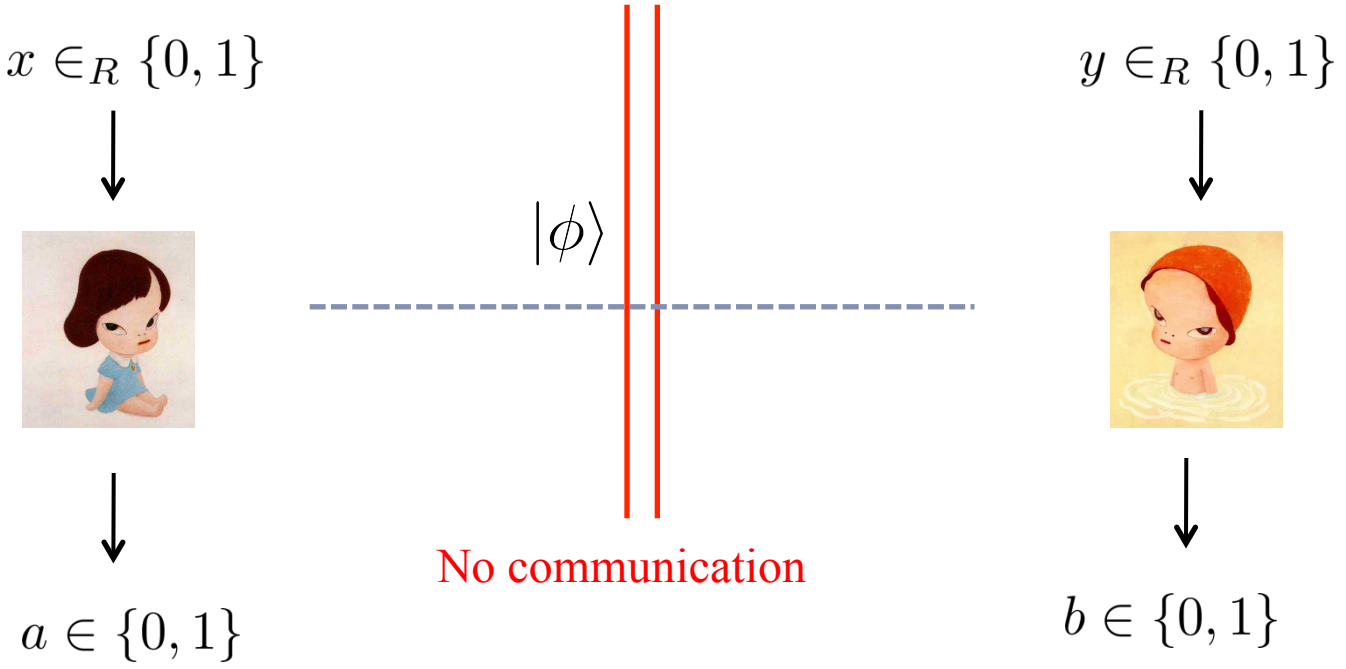
Is this notion useful ?

- Can we bound $\omega^*(G)$ using this notion of information cost ?
- At least, we want:

$$\text{if } \omega^*(G) < 1 \text{ then } \mathrm{IC}(\mathrm{G}) > 0$$

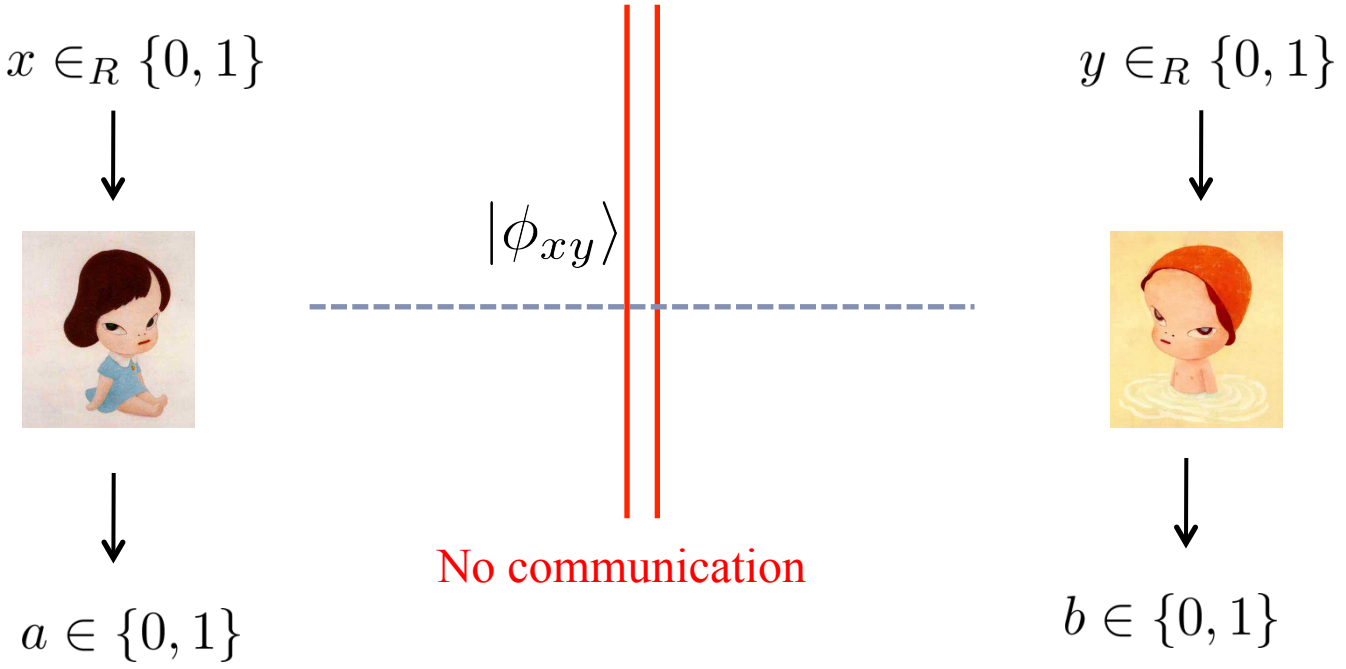
- Is that the case ? NO
- Example: CHSH game

CHSH Game



- Alice and Bob win iff. $a \oplus b = x \cdot y$
- They can win wp. at most $\omega^*(CHSH) = \cos^2(\pi/8)$

CHSH Game with advice states



- Consider the following advice states

$$|\phi_{00}\rangle = |\phi_{01}\rangle = |\phi_{01}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\phi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

- Measure in the computational basis: win wp. 1
- Alice has no information about y, Bob has no information about x.
- The information cost useless when studying games.

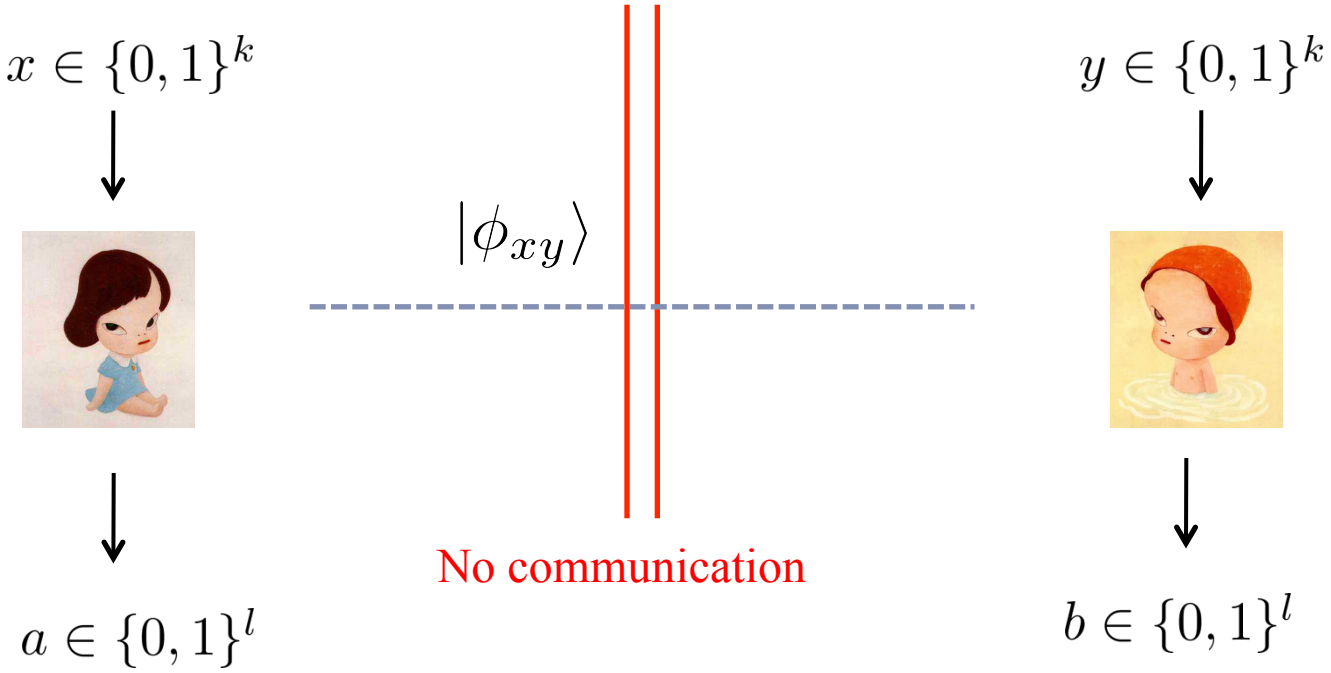
The end ?

- We wanted to extend the notion of information cost to entangled game.
- The notion we defined is pretty useless when studying entangled games.

Not yet

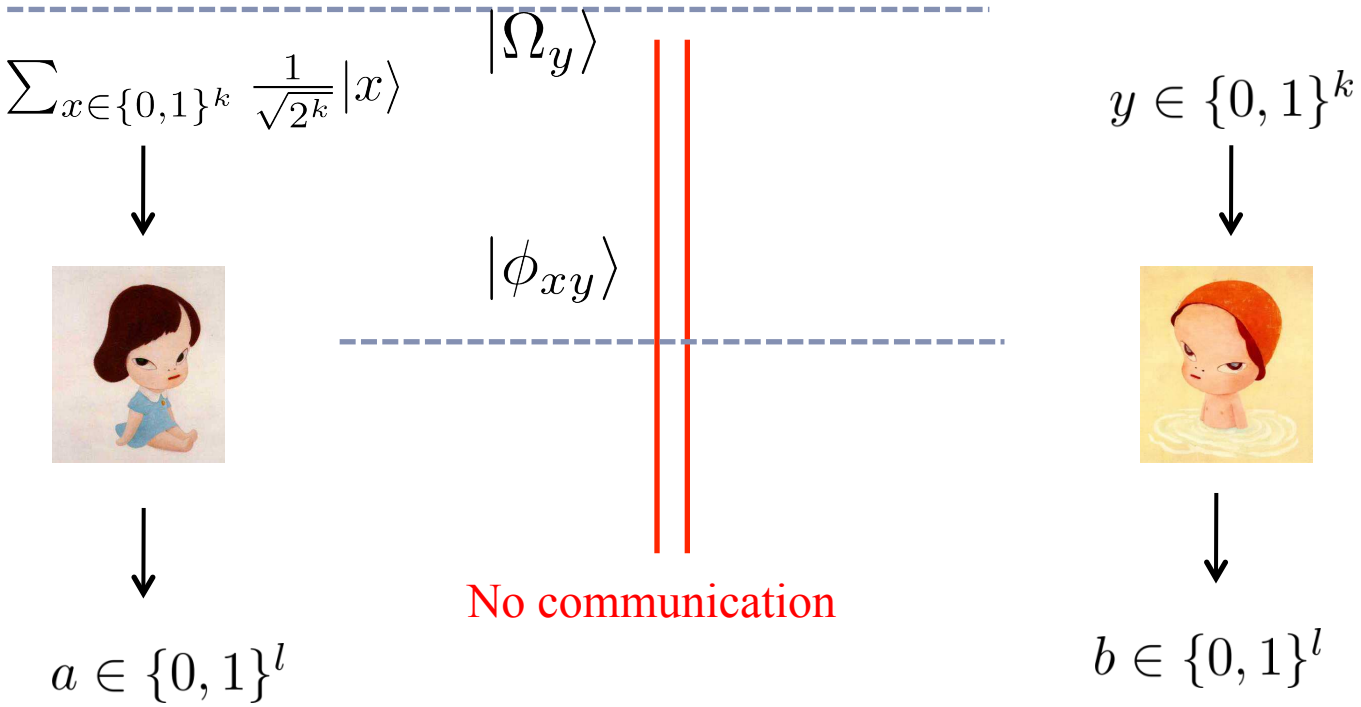
- We wanted to extend the notion of information cost to entangled game.
- The notion we defined is pretty useless when studying entangled games.
- We really really want this kind of approach to work.
  - Appealing to use information theory for entangled games
- So we cheat a bit.
- Main idea: allow the players to have a quantum superposition of their inputs.

Normal inputs



- If Bob has y, Alice has $\rho_y^A = Tr_B(\sum_{x\in\{0,1\}^k} \frac{1}{2^k}|x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}|)$

Superposed Alice



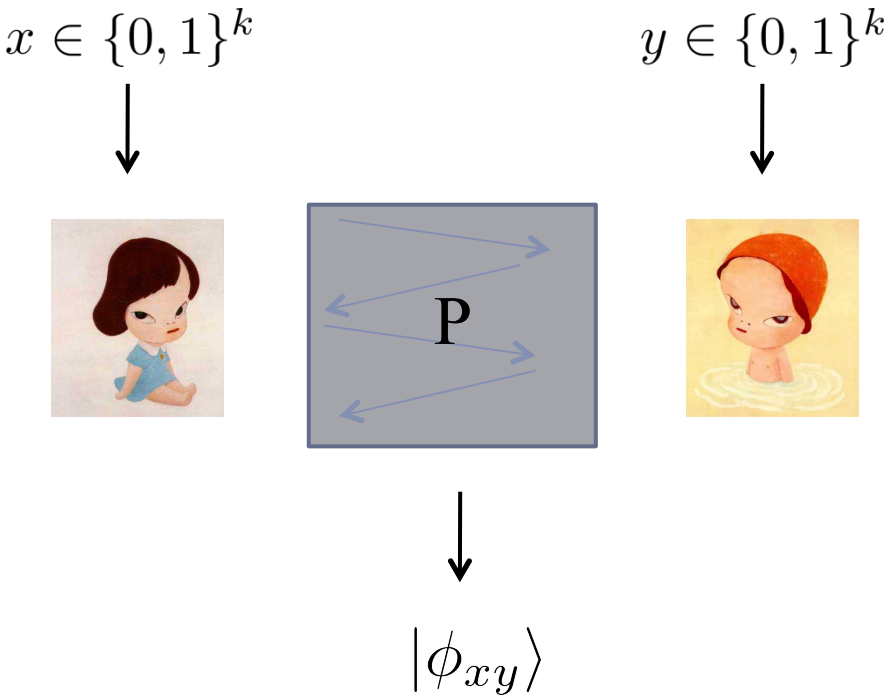
- If Bob has y, Alice has $\rho_y^A = Tr_B(\sum_{x\in\{0,1\}^k} \frac{1}{2^k}|x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}|)$
- Alice has a superposition of her inputs: If Bob has y, Alice has

$$\sigma_y^A = Tr_B(|\Omega_y\rangle) \text{ where } |\Omega_y\rangle = \frac{1}{\sqrt{2^k}} \sum_x |x\rangle|\phi_{xy}\rangle$$

- There is entanglement between Alice's superposed input and the advice.

The Superposed information cost: motivation

- Why consider superposed inputs ?



- How much about y (or x) does this procedure give away ?
- Better if secure also vs. Alice is she decides to have a superposition of her inputs.
- Arises in quantum cryptography.

The Superposed information cost

IC(G) = minimal amount of information that advice states have to give to Alice & Bob about each other's inputs to win wp. 1 ?

- Extend this the case where Alice and Bob can have a superposition of their inputs

SIC(G) = minimal amount of information that advice states have to give to superposed Alice & superposed Bob about each other's inputs to win wp. 1 ?

- Is this notion more useful ?

CHSH Game with advice states: superposed information.

- Advice states

$$|\phi_{00}\rangle = |\phi_{01}\rangle = |\phi_{01}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad |\phi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

- Recall $\rho_y^A = Tr_B(\sum_{x\in\{0,1\}} \frac{1}{2}|x\rangle\langle x| \otimes |\phi_{xy}\rangle\langle\phi_{xy}|)$ and

$$\sigma_y^A = Tr_B(|\Omega_{xy}\rangle) \text{ where } |\Omega_{xy}\rangle = \frac{1}{\sqrt{2}}\sum_x |x\rangle|\phi_{xy}\rangle$$

- Normal Alice: For each y, $\rho_y^A = \frac{I}{4}$: no info about y

- Superposed Alice: $\sigma_0^A = |+\rangle\langle+| \otimes \frac{I}{2} \quad \sigma_1^A = \frac{1}{2}|\Phi^+\rangle\langle\Phi^+| + \frac{1}{2}|\Psi^+\rangle\langle\Psi^+|$

With $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

- $\sigma_0^A \neq \sigma_1^A$: Superposed Alice has some information about Bob's input y.

The Superposed information cost: Definition

- Alice and Bob share $\rho = \frac{1}{2^{2k}} \sum_{x,y \in \{0,1\}^k} |x\rangle\langle x|_{\mathcal{X}} \otimes |\phi_{xy}\rangle\langle\phi_{xy}|_{\mathcal{AB}} \otimes |y\rangle\langle y|_{\mathcal{Y}}$

- $\sigma^A = \frac{1}{2^k} \sum_y |\Omega_y^A\rangle\langle\Omega_y^A| \otimes |y\rangle\langle y|$ where $|\Omega_y^A\rangle = \frac{1}{\sqrt{2^k}} \sum_x |x\rangle|\phi_{xy}\rangle$

↓

The state that A & B share if Alice has a superposition of her inputs

- $\sigma^B = \frac{1}{2^k} \sum_x |x\rangle\langle x| \otimes |\Omega_x^B\rangle\langle\Omega_{xy}^B|$ where $|\Omega_x^B\rangle = \frac{1}{\sqrt{2^k}} \sum_y |\phi_{xy}\rangle|y\rangle$

- $SIC(\rho) = I(Y : XA)_{\sigma^A} + I(X : BY)_{\sigma^B}$

↓

Information that Alice has about Bob's input when they share σ^A

The Superposed information cost: Definition

- Superposed information cost of a game

Definition: $SIC(G) = \inf_\rho SIC(\rho)$

Where the inf. is taken over states ρ st. Alice & Bob win G wp. 1 using ρ

- ρ is of this form $\rho = \frac{1}{2^{2k}} \sum_{x,y \in \{0,1\}^k} |x\rangle\langle x|_{\mathcal{X}} \otimes |\phi_{xy}\rangle\langle\phi_{xy}|_{\mathcal{AB}} \otimes |y\rangle\langle y|_{\mathcal{Y}}$

Upper bounding SIC(G^n)

- Additivity: $SIC(G^n) = nSIC(G)$
  - Almost for free because the information cost is a nice IT quantity.

- Relation to $\omega^*(G)$: $SIC(G) \geq \frac{1-\omega^*(G)}{32\ln(2)}$
  - One of the main ingredients of the proof.
  - Shows that the notion of SIC is interesting for games.

- Putting this together $SIC(G^n) \geq \frac{n(1-\omega^*(G))}{32\ln(2)}$
  - It's a hint that it's hard to win G^n but it's not an actual proof

How do we show parallel repetition ?

- Let t that satisfies $\omega^*(G^n) = 2^{-t}$. We show that $t \geq f(n)$ for some function f.

- We show that $SIC^1(G^n) \leq \frac{t \cdot kl}{1-\omega^*(G)}$

1: we don't use exactly SIC but the spirit is there.

How do we show parallel repetition ?

- Let t that satisfies $\omega^*(G^n) = 2^{-t}$. We show that $t \geq f(n)$ for some function f.
- We show that $SIC^1(G^n) \leq \frac{t \cdot kl}{1-\omega^*(G)}$
- We had $SIC(G^n) \geq \frac{n(1-\omega^*(G))}{32\ln(2)}$
- Putting it all together, we get $t \geq \frac{n(1-\omega^*(G))^2}{32\ln(2)kl}$ which gives

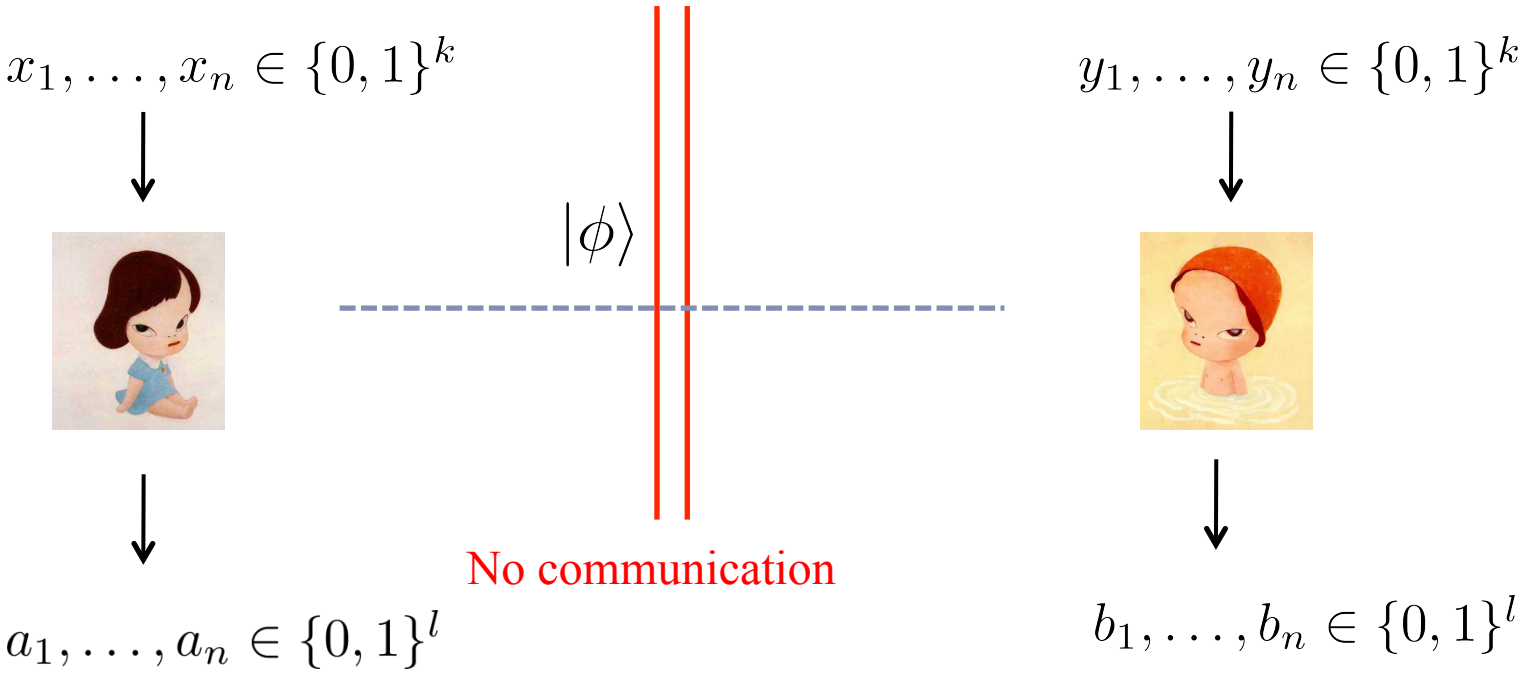
THEOREM

For any game G on the uniform distribution such that $\omega^*(G) \leq 1-\varepsilon$, we have $\omega^*(G^n) \leq (1-\varepsilon^2)^{\Omega(\frac{n}{kl})}$

1: we don't use exactly SIC but the spirit is there.

Intuition on why $SIC(G^n) \leq \frac{t \cdot kl}{1-\omega^*(G)}$

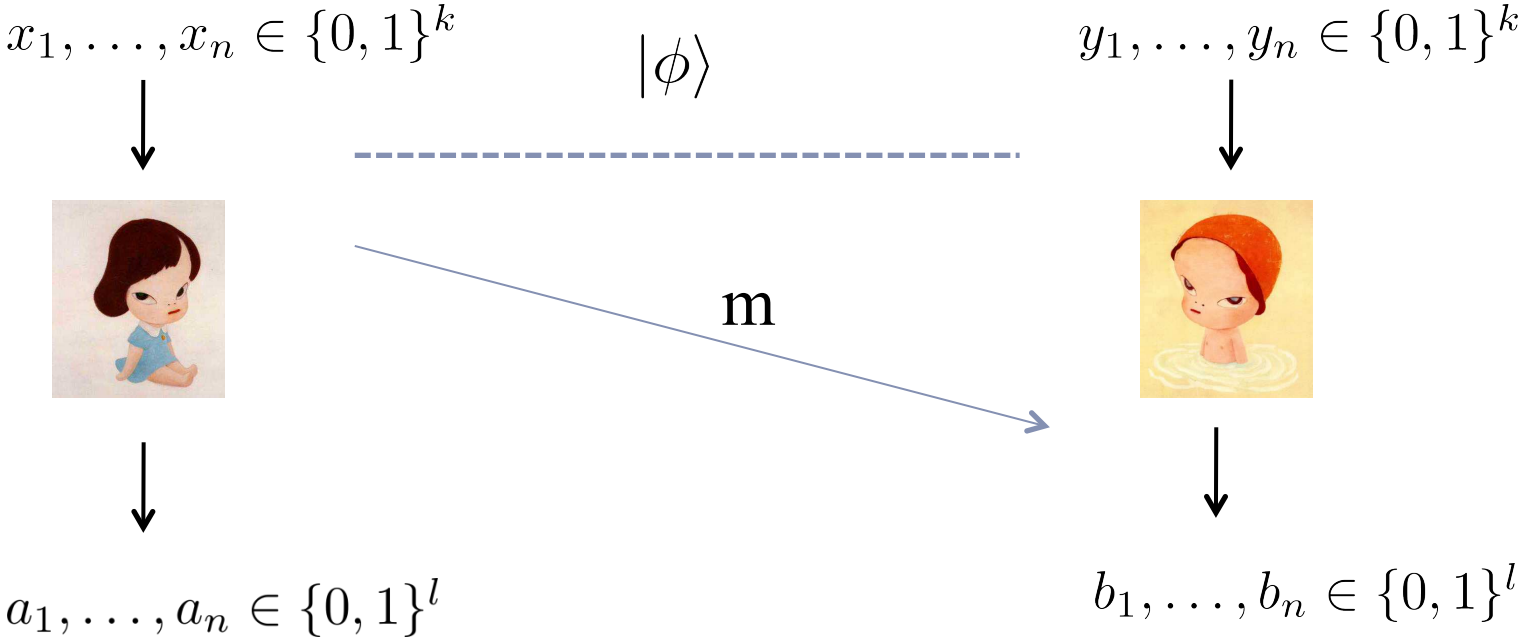
- Recap: we start from G^n.



- We want to show that $SIC(G^n) \leq \frac{t \cdot kl}{1-\omega^*(G)}$

Intuition on why $SIC(G^n) \leq \frac{t \cdot kl}{1-\omega^*(G)}$

- Communication protocol



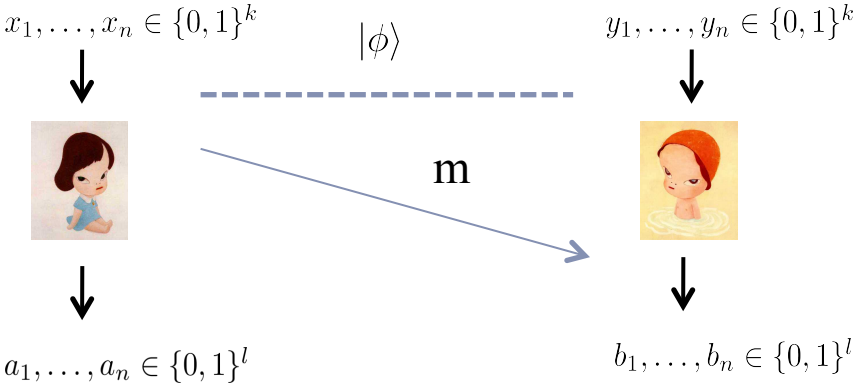
- What amount of bits Alice has to send to Bob st. Alice & Bob win wp 1 ?

The communication protocol

- This question is a hard question. We show a much weaker statement.
- Alice can send $m = O(\frac{t \cdot kl}{\varepsilon})$ to Bob.
- After the message
  - The probability of winning G^n doesn't increase
  - But: Bob knows whether they win the game.
- That will be enough.

The communication protocol

- How do they do ?



- Alice and Bob play the game optimally G^n
  - They can win wp. $\omega^*(G^n)$
- Alice picks $O(\frac{t}{\varepsilon})$ random pairs of input/output (x_i,a_i) and sends them to Bob
- Bob checks for each of these pairs that $V(a_i, b_i|x_i, y_i) = 1$
  - If this holds for each pair, Bob knows that they win G^n with high pr.

The communication protocol

- Alice sends $O(\frac{t}{\varepsilon})$ pairs each of size kl so $m = O(\frac{t \cdot kl}{\varepsilon})$
- Let ξ the state that Alice and Bob share conditioned on winning.
  - This state is created by sending $m = O(\frac{t \cdot kl}{\varepsilon})$ + postselection so it doesn't have high SIC, $SIC(\xi) = O(\frac{t \cdot kl}{\varepsilon})$
  - This state allows the players to win G^n wp. 1
  - This means that $SIC(G^n) = O(\frac{t \cdot kl}{\varepsilon})$
  - The above 3 statements are almost true but that's ok.

How do we show parallel repetition ?

- Let t that satisfies $\omega^*(G^n) = 2^{-t}$. We show that $t \geq f(n)$ for some function f.
- We show that $SIC^1(G^n) \leq \frac{t \cdot kl}{1-\omega^*(G)}$
- We had $SIC(G^n) \geq \frac{n(1-\omega^*(G))}{32\ln(2)}$
- Putting it all together, we get $t \geq \frac{n(1-\omega^*(G))^2}{32\ln(2)kl}$ which gives

THEOREM

For any game G on the uniform distribution such that $\omega^*(G) \leq 1-\varepsilon$, we have $\omega^*(G^n) \leq (1-\varepsilon^2)^{\Omega(\frac{n}{kl})}$

1: we don't use exactly SIC but the spirit is there.

Conclusion

- We introduced the Superposed Information Cost, a powerful tool for the study of entangled games.
- We managed to use this notion to prove parallel repetition for entangled games.

- Can we remove the assumption on the inputs ?
- Can we use this tool for other problems related to entangled games or quantum communication complexity ?